Komentarz KBN

Nr 6 (109) / 2023 13 kwietnia 2023 r.

The Goals of the Russian (Cyber)Gray Zone Activities in Ukraine

Dominika Dziwisz

Introduction

International conflicts arise from contradictory interests that accumulate over time, and gray zone activities can be seen as part of a larger conflict cycle that can lead to both escalation and de-escalation. A well-managed conflict in the gray zone should be able to produce strategic outcomes, but in the case of the Russia-Ukraine conflict it has gone way beyond the gray zone. The shift from a gray zone to open conflict in Ukraine offers new perspectives for examining to what extent countries may utilize and compete in the gray zone in the future, and about the levels of the threshold of aggression.

On February 24th, 2022, the International Institute of Strategic Studies released a comparative report analyzing the offensive cyber operations of the United States, Russia, and China, coinciding with the beginning of the Russia-Ukraine war. The report found that the United States is well equipped to project power through cyberspace thanks to its organizational resources and structure. In contrast, Russia possesses strong foundations for cyber-sabotage and cyber-influence operations but has been hindered by limited resources and narrow transformations within relevant agencies. China has demonstrated interest in using cyberspace to project power for social and political purposes, particularly with regard to Taiwan, though these operations have thus far been largely disruptive in nature. Despite their varying degrees of offensive cyber capabilities, all three nations share a common concern at the political level regarding the low confidence in the

ability of cyber campaigns to achieve strategic impact. However, one could speculate whether Russia's employment of cyberspace during the conflict in Ukraine sets it apart from Western nations in comprehending the use of cyberspace for strategic goals. This raises three fundamental questions: What were Russia's objectives for leveraging the (cyber)gray zone? To what extent do Western specialists possess a comprehensive understanding of Russia's cyberspace utilization? Lastly, how can the lessons learned from the ongoing conflict between Russia and Ukraine shape our future strategies in effectively dealing with the challenges of the gray zone?

Russia in the Gray Zone

At the 2013 meeting between high-ranking Russian and American defense officials, General Nikolai Makarov derided the absence of information warfare in the mission of the US Cyber Command (USCYBERCOM). In his inflammatory address, he asserted that "information is used to destroy nations, not networks", suggesting that the US's disregard for information warfare demonstrated its ignorance. This was also a distinct signal regarding Russia's cyberspace priorities, which were subsequently mirrored in Russian strategic papers and deployed in Ukraine since at least the Crimea annexation.

From 2014 to February 2022, Russia pursued a gray zone conflict strategy, including activities in cyberspace, to pressure Kyiv into making concessions. Various cyber-tools, such as ongoing misinformation and disinformation, propaganda, election interference in 2014, cyberattacks on critical infrastructure in 2015, and a cyberattack on Ukraine's ministries and banks in February 2022, were employed in a limited military competition that persisted beyond peace but stopped short of a full-scale war. The goal of all these actions was to avoid open conflict and serious clashes while still achieving strategic objectives. Therefore, it can be concluded that the Russia-Ukraine conflict before February 24th, 2022, was a perfect example of "salami tactics".

After witnessing Russia's achievements in the gray zone, certain experts suggested that Russia could accomplish comparable goals in Ukraine without resorting to military action by solely relying on cyberattacks. This approach ultimately failed. Despite the conflict's current hot phase, specialists concur that cyber-attacks have not yielded remarkable breakthroughs on the battlefield. Furthermore, few of the projected connections between cyber and military operations have transpired as anticipated. In contrast to initial attempts to combine cyber and kinetic forces, we now observe the separate use of these two capabilities by Russia. This could result from distinct goals established for the Russian cyber and kinetic invasion, with cyber focused on information warfare and kinetic operations aimed at territorial acquisition. While cyberweapons are seen by Russians as insufficient for the complete takeover of a nation, they are still considered a potent tool for competing in the information sphere and achieving political goals. However, when it comes to capturing territory, kinetic forces are viewed as a more dependable option.

Taming World Opinion Strategy

It can be assumed that the Russian cyber gray zone had three fundamental objectives:

1. Creating circumstances that lead to crises – primarily by identifying vulnerabilities in critical infrastructure facilities and launching attacks, such as the 2015 power grid hack, a significant cyber attack that resulted in the widespread power outage in Ukraine.
2. Evaluating the response of Western nations to these attacks.
3. Spreading misinformation and propaganda.

All of these activities were bounded by the overwhelming goal which was taming the world opinion and slowly getting us used to the situation in Ukraine. The primary objective of all these activities was to shape global opinion and gradually acclimate us to the situation in Ukraine. Putin's pre-war tactics can be compared to the parable of the frog in boiling water, where a situation worsens gradually, leading to the lethal danger without realizing this, until it is too late. Putin skillfully reduced the West's vigilance, and cyber tools proved to be an ideal way to achieve this goal. This is primarily due to three features of cyberspace: the challenge of tracing attacks to their source, lack of territorial boundaries, and the ease of disrupting an adversary's information exchange.

Therefore, Russia was able to exploit the lack of resolve among NATO countries by utilizing the "taming world opinion strategy". Within the gray zone, the Russians launched cyberattacks that could be viewed as hostile acts of aggression against Ukraine, such as the 2015 power grid hack, the 2017 NotPetya attack, and the 2022 Viasat attack. The challenge did not lie in identifying the source of these attacks, but rather in lacking the necessary resolve to respond to them. Ultimately, determining what actions constitute aggression under international law is always a matter of political judgment. In fact, the use of the term "gray zone" by decision makers may reflect their reluctance to label certain actions as "war". However, this does not imply that all forms of aggression should be classified as war; the decision ultimately rests with those in power.

During the ongoing phase of the war, Russia has persisted in utilizing cyberspace for carrying out operations in the gray zone against countries that support Ukraine. Therefore, it can be anticipated that there will be an escalating intensification of disinformation and intelligence operations. This is supported by the statements of Microsoft specialists who suggest that Russian hostile activities against Ukraine-supporting countries are predominantly related to intelligence. This includes attempts to obtain knowledge about the logistics of supplying aid to Ukraine, as well as efforts directed at Ukraine-supportive nations, which were not designed to cause harm to systems, but rather to gather information.

Conclusions

The objectives of Russia's gray zone activities in Ukraine from 2014 to 2022 were centered around controlling global opinion. By using cyberattacks and propaganda to gradually erode Western vigilance, Putin aimed to get the West used to the situation in Ukraine. This strategy proved successful due to the lack of determination among NATO countries and the fact that decision makers were reluctant to classify these attacks as “war”. Russia took advantage of NATO countries' lack of determination, rather than the difficulty of attributing the attacks. When the decision on

what constitutes aggression according to international law is ultimately a political one, the problem lies in the lack of political will to act. This created a gray zone in which Russia could operate. Therefore, to counteract gray-zone activities, the key requirement is resolve rather than merely stronger attribution or better laws.

As the ongoing war demonstrates, the advantages of cyber operations in the gray zone have become less significant as the conflict escalates. The key advantage of cyber activities, which is the problem of attribution, becomes less relevant when both parties are engaged in physical confrontation and their intentions are clear. The second advantage, which is the ease of disorganizing the enemy's information exchange, can be achieved more effectively through missile attacks on ICT infrastructure. Lastly, the third advantage of cyber operations – non-territoriality – loses its significance when targets can be attacked throughout the enemy territory with kinetic means, as the Russians do in Ukraine.

Citation: Dominika Dziwisz, 'The Goals of the Russian (Cyber)Gray Zone Activities in Ukraine', *KBN Commentary* 2023, no. 6 (109), 13 April.